Window Security Enhancements

Windows & Linux Security Comparison Instructions:

1. Look at how the two systems implement log-on security. Although both systems can use password protection to prevent unauthorized users from logging on the system, Windows allows user and administrative accounts to be created without requiring a password.
2. Look at how the two systems deal with administrative user access (root user in Linux). Although it varies by Linux distribution, most prevent even administrative users from running software as root without password verification. Windows runs all software in administrative accounts as root and defaults to administrator for new users.
3. Look at the track record for malicious software. Most malware, a term that includes viruses and spyware, is targeted at Windows-based systems. Very few instances of malware designed for Linux systems have been found.
4. Examine the track record for critical security flaws under both systems. According to an article in The Register, the U.S. Computer Emergency Readiness Team (CERT) lists 39 of the first 40 flaws in Microsoft Windows as "critical." Only three of the first 40 queries for Red Hat Linux were listed as "critical."
5. Look at firewall security on both systems. Windows now comes with firewall capabilities built in. Although the firewall leaves certain ports visible to the network, it closes the ports. Linux doesn't come with a firewall pre-installed. However, if you don't install servers on your Linux desktop, Linux will not even report the existence of various ports. If you decide to install one of many Linux firewalls, you can configure it to not report the existence of certain ports, leave certain ports open for connection and leave others completely closed. Linux firewalls are far more configurable than those running on Windows. Unless you understand TCP/IP networking, however, this can be a double-edged sword. Without proper knowledge, it is much easier to misconfigure Linux firewalls.

Introduction Windows Vista Security

Windows Vista is officially available, so we thought it was time for you to get to know this new operating system. Here are five security features in Windows Vista that might just surprise you:

1. **Check your spyware protection through the Windows Security Center.** If you've used Windows XP, then you already know about Windows Security Center, the all-in-one monitoring tool that helps you keep track of your firewall, automatic updates, and antivirus software. Windows Security Center for Windows Vista has more security categories. It now warns you if your antispyware software is not up and running like it should be.
2. **Help prevent identity theft with Phishing Filter.** Windows Vista comes with Phishing Filter, which is built in to Internet Explorer 7. You just need to turn it on.

The filter checks Web pages before you connect to them and warns you about sites that have typical characteristics of fraudulent Web sites designed to steal your identity, sometimes called phishing scams. The filter is updated several times an hour using the latest security information from Microsoft and several industry partners. This can help you avoid identity theft from phony sites that might look, for example, like your bank's site.

3. **New junk mail filter for Windows Mail.** Windows Mail, the new e-mail program that comes with Windows Vista, helps reduce the risks of junk mail and scams. In fact, Windows Mail comes with a junk e-mail filter that until now has been available only in Microsoft Office Outlook.
4. **Track what your children are doing online.** If you're a parent, you already know how important it is to have open communication with your children about their computer use. You might also want to review what your child is doing online. With Windows Vista, you can create activity reports that provide details of how your children have spent their time on the computer, including the Web pages they've visited, programs they've used, and games they've played.
5. **Find security tools faster.** When you want to change settings on the security tools in Windows Vista, there's no need to dig through the Start menu or the control panel. Simply type "Windows Security Center," "Phishing Filter," "Parental Controls," or any other program or file into the Instant Search box on the Start menu and then select it from the programs list.

Windows Vista can help protect your PC and the people who use it by providing improved safety and security features so you can use your computer with confidence.

1. **BitLocker Drive Encryption**
   BitLocker Drive Encryption is a security feature that provides better data protection for your computer by encrypting all data stored on the Windows operating system volume. BitLocker Drive Encryption is available in Windows Vista Enterprise and Ultimate for client computers and in Windows Server 2008. Both business and personal users can turn on BitLocker Drive Encryption to help protect sensitive data on their PCs.
2. **Encrypting File System**
   Encrypting File System, available in Business, Enterprise, and Ultimate editions of Windows Vista, is useful for user-level file and folder encryption. For example, if two users are sharing a computer, an administrator can use Encrypting File System to encrypt each user's data to make it unavailable to the other user. For network file and folder encryption, Windows Vista enables administrators to store Encrypting File System keys on smart cards.
3. **Parental Controls**
   The parental controls built into Windows Vista help parents determine which games their children can play, which programs they can use, and which websites they can visit—and when. Parents can restrict computer use to specific times and trust that Windows Vista will enforce those restrictions, even when they're away from home.

4. **Shadow Copy**
   Available in the Ultimate, Business, and Enterprise editions of Windows Vista, this feature creates point-in-time copies of files as you work, so you can retrieve versions of a document you may have accidentally deleted. Shadow copy is automatically turned on in Windows Vista and creates copies, on a scheduled basis, of files that have changed. Since only incremental changes are saved, minimal disk space is used for shadow copies.
5. **User Account Control**
   User Account Control in Windows Vista helps prevent potentially harmful software from making changes to your computer without your explicit consent. This feature works with Windows Defender, Internet Explorer 7, and Internet Explorer 8 to help reduce the impact of viruses, spyware, and other threats. With User Account Control and the Parental Controls in Windows Vista, you can create a separate account for each member of the family and control which websites, programs, and games each person can use and install.
6. **Windows Backup and Restore Center**
   The file backup and restore features in Windows Vista help you keep your data safe from user error, hardware failure, and other problems. Windows Backup and Restore Center gives you one place to manage all backup and restore features. Depending on the version of Windows Vista you have, there are two approaches you can take to backing up files: Automatic Backup, which backs up just your files and data; or Complete PC Backup, which backs up everything on your PC, including the operating system and applications.
7. **Windows Defender**
   Windows Defender is antispyware software that can help protect your computer against spyware and other potentially unwanted software. Windows Defender works with Internet Explorer 7 and Internet Explorer 8 and comes with preconfigured settings and guidance to help you get and stay secure.
8. **Windows Firewall**
   Windows Firewall helps you protect your computer against many types of malicious software by restricting other operating system resources if they behave in unexpected ways—a common indicator of the presence of malware. Properly configured, it can stop many kinds of malware before they can infect your computer or other computers on your network. Windows Firewall, which comes with Windows Vista, is turned on by default and begins protecting your computer as soon as Windows starts. The Windows Firewall Control Panel is designed to be easy to use, with several configuration options and a simple interface.
9. **Windows Security Center**
   Windows Security Center helps make your PC secure by alerting you when your security software is out of date or when your security settings should be strengthened. The Security Center displays your firewall settings and tells you whether your PC is set up to receive automatic software updates from Microsoft. Windows Security Center also shows the status of software designed to protect against spyware, your Internet Explorer 7 or Internet Explorer 8 security settings, and User Account Control. In addition, Windows Security Center can monitor

security products from multiple companies and show you which are enabled and up to date.

10. **Windows Update**

    Windows Update helps keep your computer current and secure by automatically downloading and installing the latest security and feature updates from Microsoft. Windows Update determines which updates are applicable to your computer and can download and install them automatically to keep your computer up to date and more secure. To make sure your computer stays up to date, you should set up your system to install updates automatically. This helps ensure that both Important and Recommended updates are downloaded and installed in Windows Vista.

Introduction Windows 7 Security

Windows 7 is Microsoft's latest desktop-based client operating system which builds on the strengths and weaknesses of its predecessors, Windows XP and Windows Vista. Every aspect of the base operating system as well as the services it runs and how it manages the applications loaded within it has been reviewed and made more secure if possible. All services have been enhanced and new security options making it more reliable. Aside from basic system enhancements and new services, Windows 7 delivers more security functionality, enhanced auditing and monitoring capabilities and the ability to encrypt remote connections and your data, Windows 7 also has newly developed internal protection enhancements to secure system internals such as Kernel Patch Protection, Service Hardening, Data Execution Prevention, Address Space Layout Randomization, and Mandatory Integrity Levels.

Windows 7 is designed to be used securely. For one, it was developed Microsoft‘s Security Development Lifecycle (SDL) framework and engineered to support Common Criteria requirements allowing it to achieve Evaluation Assurance Level (EAL) 4 certification which meets Federal Information Processing Standard (FIPS) #140-2.When used as a stand-alone system, Windows 7 can be secured for personal security. Windows 7 has many helpful security-based toolsets contained within, but it is only when Windows 7 is used with Windows Server 2008 (R2) and Active Directory, that it turns into a bullet-proof vest. By leveraging additional security from tools such as Group Policy, you can control every aspect of desktop security. If Windows 7 is used mainly for your home office or personal use, it can still be secured to prevent many current methods of hacking and attacking and can be restored quickly if disaster does in fact strike, so although beneficial, Windows 2008 is not completely necessary to apply a high level of security to Windows 7. You should also consider that Windows 7 is inherently secure, but it does not necessarily mean that you should rely on the default configuration without making any adjustments to extend your security coverage. You should also consider that you will eventually be subjected to some form of malware or Internet-based attack when the computer is being utilized on any public network. If a computer is used for any type of public Internet access, your system and the network on which it is connected, becomes opened up to possible attack.

In this article, we will cover the fundamentals you need to know to secure Windows 7 correctly, achieve a baseline level of security, review advanced security configurations and explore some of the lesser known security functionality Windows 7 provides in order to prevent or protect against a possible attack. We will also look at the many ways you can safeguard your data and get back up and running quickly if you do in fact suffer from some form of attack or catastrophic system malfunction you cannot recover from. This article introduces the concepts of security, how to harden Windows 7, how to install and provide security for your running applications, how to manage security on a Windows 7 system and how to prevent the problems caused by malware. This article also covers the process of safeguarding your data, the backup and recovery operating system features, how to restore your operating system to a previous state and ways to recover you data and

system state if a disaster does occur. We also cover strategies to do it quickly. Topics are also covered on how to work safely while working online or over the Internet, how to configure biometric control for advanced access control and how Windows 7, and when used with Windows Server 2008 (and Active Directory), how you can securely integrated more options for control, management and monitoring. The goal of this article is to familiarize you with Windows 7 security features, enhancements and their application as well as to give you some insight on how to plan for and apply these security features correctly. The concepts we cover are divided up and organized in a building-block approach.

PolicyKit for Window 7

Even riskier is the number of times we resort to typing sudo or launching a shell with administrator privileges, effectively bypassing the security inherent in the normal/root user system. Many distributions and developers think there needs to be an extra level of security, and the closest we can get to the technology behind Microsoft's UAC is PolicyKit, originally developed by Red Hat but now shipped as standard in Fedora, OpenSUSE and Ubuntu. PolicyKit gives application developers (and distribution builders) a finer degree of control over what an application can and can't do while it's running. It could enable a user to mount portable storage, for instance, but not allow the same user to mount a local filesystem, avoiding the potential hazard of sudo completely.

The impending KDE 4.3 includes PolicyKit integration, which means that many system administration applications for the KDE desktop will be able to take advantage of PolicyKit's finer-grained privilege control in much the same way that certain applications request authentication on the OS X desktop. Gnome has had this functionality since the beginning of last year, and its inclusion in KDE brings us a step closer to a unified desktop on the Linux platform and a unified system for accessing administrative tasks.

Online security

Despite all these improvements to User Access Control, Windows is still going to be the main target for hackers, and as such, a virus checker is always going to be necessary. For the first time, Microsoft is going to bundle a virus checker and spyware detector with the operating system. This is likely to raise considerable protest from manufacturers who sell competing products, such as Symantec and McAfee, as they're making a tidy living from plugging this lucrative hole in current Windows security. But bundling a free virus checker with the operating system is a great step forward for the rest of us who have to endure a constant stream of attacks from compromised Windows systems. Microsoft's checker is going to be part of the 'Security Essentials' download package, and it replaces Windows Live OneCare, a similar package that Microsoft previously charged for on XP and Vista.

Microsoft's Security Essentials covers only the basics of online security: real-time virus checking, system monitoring and download scanning. This should leave plenty of room for the commercial solutions to fight over more advanced features and neurotic Windows

users. As Linux users, we don't need to run a virus-checker unless you're receiving files from, and sending them to, Windows users. It avoids the extra CPU and memory load of constantly running a checker and keeping it up to date. But there are several checkers that are up to the task if you need them, including tools from BitDefender and AVG, as well as the excellent ClamAV.

Basic Security Considerations

Before we dig into the specifics of Windows 7, it is important that we first introduce the basic concepts of security and how to plan for the application of it. We will also need to know why monitoring is crucial to maintain security and how to correctly monitor security services for problems. It is also important to know how to monitor security and discover if you are open to a potential attack. Security is not something you haphazardly plan for and then quickly apply. It is a concept that must be applied to every technical aspect of your deployment, as well as a practice to live by. It is also something that must be thought out well before deployment and then monitored and managed after it is applied. Managing security requires analysis work to fine tune the current security architecture, as well as to uncover potential attacks. Most times, your security will be tested by an attacker or malicious program to find access and in this process; you can potentially protect yourself proactively if you can see the attempts and do something about it. Through logging and then auditing, you can find out information about what is querying your router login prompts, administrator account login attempts and more.

Logs and alerts are helpful so that when something does go wrong, you can react to it quickly and correctly via analyzing source IP addresses, or attempts at login caught by auditing. Responding to an attack with a detailed plan is called ‘incident response’. Being prepared is the key to incident response so having a proactive plan and reactive plan are critical to have in place before disaster strikes. A Disaster Recovery Plan [sometimes used in combination with a Business Continuity Plan (BCP)], will contain a strategy for recovering from incidents. Some IT teams also have IT professionals assigned to what is called an ‘Incident Response Team’, which when activated, is responsible for following the laid out plan in order to fix and resolve critical issues that results in major system downtime, or worse, data loss, network and systems attacks and more.

So, for home users and stand alone systems, you should follow this same strategy but at a simplified level. You still need to secure things, and react to disaster, so a good plan created in advance to the disaster will go a long way in getting you back on your feet quickly. A good example of a simple plan would be, if your system becomes infected with a malware (such as a Trojan), you may have to reinstall the operating system if all other restoration and repair attempts fail. If that is the case, then you need assigned team members, detailed steps (or a checklist) and procedures in place before the disaster so that you can react to it correctly and a testing process to ensure that everything is done correctly after recovery takes place. Having access to, or a copy of the installation files or any other programs and applications in place beforehand saves time and the plan, if set up correctly, can point you in the right direction towards all the tools you need when the clock starts counting down.

To help you plan and become more knowledgeable about security, you can find checklists and plans in the Reference Links section of this article. You should also revisit your plans often, especially after a critical issue or outage, with action items added if needed. Once your plan is in place, you should consider building upon your foundation with more security functionality and services.

Security should be considered and applied to any system or service in use so that you can mitigate the risks associated with attacks coming from any one of them while in use. And if security is applied in a way that you can proactively prevent (or recover from) an attack or disaster of any kind from occurring in the first place, you have less to react to and manage. Security, even at its most basic application level must be applied in order to keep your personal data secure so that if you do need to completely reinstall Windows from scratch, you can re-apply your data afterwards so that it can be accessed and utilized. Security cannot be ignored.

You should also consider deploying security both conceptually and technically using the Defense in Depth security concept. Security must be considered and applied to all systems, services, applications and network equipment, keeping your system up and running and also connected to the Internet for use. Posted policies and developed plans keep users of the systems productive, and aware of general use policies. Continued upkeep will keep your investment growing. To prevent holes in your security architecture, you must consider planning for and applying a security model that utilizes the concept of 'Defense in Depth'. Figure 1 shows the application of defense in depth at a very simplistic level, you can (and should) of course add more layers depending on how your home or corporate network is set up.

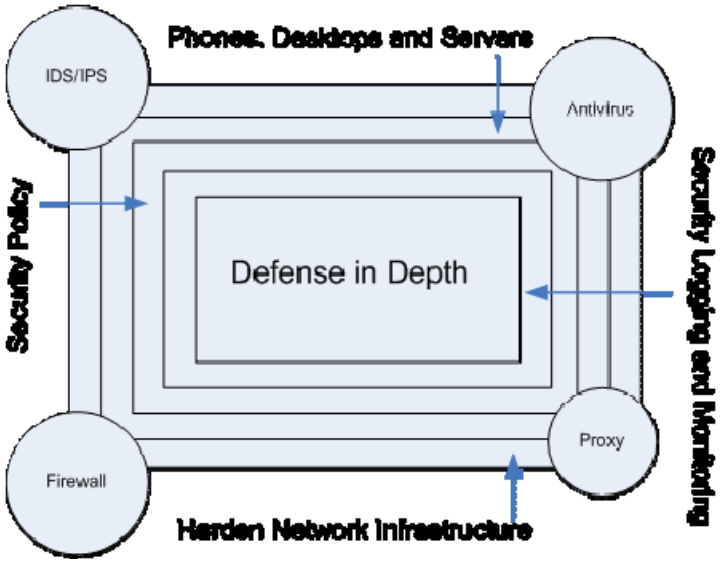

Figure 1: Viewing how Defense in Depth is Conceptualized and Deployed

Defense in Depth as seen here can be customized to your needs. In this example, a security policy is needed to provide security-based direction and communication to the users of the systems and network. Also, hardening your systems, phones, desktops,

services, applications, servers, routers, switches and PBX should all be considered to ensure that all points of entry are covered. It would also make sense to have some form of public Internet protection (such as a firewall) in place if in use, but always expand on that and add other items such as probes, filters and scanners for more granular support. You will also need a way to monitor and log all of this information for review if needed.

Windows 7 was also designed to be integrated and used in any environment that must comply with a high level of security, such as the U.S. Government and the U.S. Military. When considering basic Windows security principles, it's important to remember that any enterprise level system must be certified with the C2 level of security from the Orange Book. Microsoft Windows also needs to comply with the Common Criteria Certification. For more information on these topics, you can find other articles and more information at the end of this article in the Reference Links section. Windows 7 is also extremely flexible, with many options to configure a system with complete functionality (minimal security), or one locked down to the point of basic operation, and only operations you configure for use (maximum security).With Windows 2008 and Windows 7, the security functionality is increased tenfold when used together correctly.

It is important to remember that denial of a problem (or potential problem) is not an option. Problems compound when left to be taken care of later, or ignored completely. Laziness will only buy you so much time. Security through obscurity is not security. Non-compliance only causes more problems later when compliance is needed. A thorough deployment of security on your home PC, or within an enterprise (both equally important), will prevent most infiltrations and attacks and provide multiple layers of protection to keep your security posture high but not prevent them all. You need to know the fundamentals of security and how to operate both proactively and reactively to attacks if you want to be secure.

So, now that you are familiar with basic security concepts, let us apply what we learned while configuring Windows 7 security settings. Considering that we attained the knowledge of why we want to apply security, when to apply it, as well as the reasons for managing, monitoring and updating it, all we need to do is further apply those security concepts while configuring a base Windows 7 system. This is done fairly easily if you know what you need to (and want to) do. If a new user of Windows or having a hard time getting acclimated to 7 (perhaps you skipped Vista) – then it is important to spend some time navigating these tools and attempting to research them on TechNet or Microsoft Support online to learn more. For example, many templates and checklists can be found online at Microsoft.com, which give you the ability to go step by step through applying and using security on your Windows systems. You can also find helpful tools in the Reference Links section of this article.

Templates are not always the answer and can sometimes cause adverse effects if not used correctly (or configured correctly), so always use with caution - even if downloaded directly from Microsoft.com. It's important to always read the documentation that comes with the template so you can apply it correctly. It's also safe to say that, without a background in the OS itself, or knowledge of the fundamental principles in which it

operates, you will not be able to maintain a high level of security for long. An intimate understanding of the core OS and its services is needed if you want to be able to continue a high security posture even after you have configured security on your base system correctly. A good example of why this is important for anyone applying security to an OS is, one of the best ways to thwart attack is to know that you actively being scanned, or checked for exploitation. Event Viewer logging is extremely helpful, because you can configure auditing (as an example) and get detailed information on what is happening with and in within your systems. Most (if not all) logs are cryptic by nature and spell out the problem in the most basic of terms or with a handful of machine language (captured dump). You will need to go online and unravel the mystery which with some practice gets easier and easier as you continue to do so. You wind up reading a lot of things you didn't know about and finding a lot of tools that you will want to add to your kit for future deployments once tested.

You also need a level of flexibility when applying security, a level that allows you to meet business goals and requirements (such as Internet access) without problem while still maintaining a high level of security as needed. A great example is the User Account Control (UAC) tool, which when adjusted, can provide a high level of security, or be turned off completely. You will have to reboot your system if you turn off the UAC.

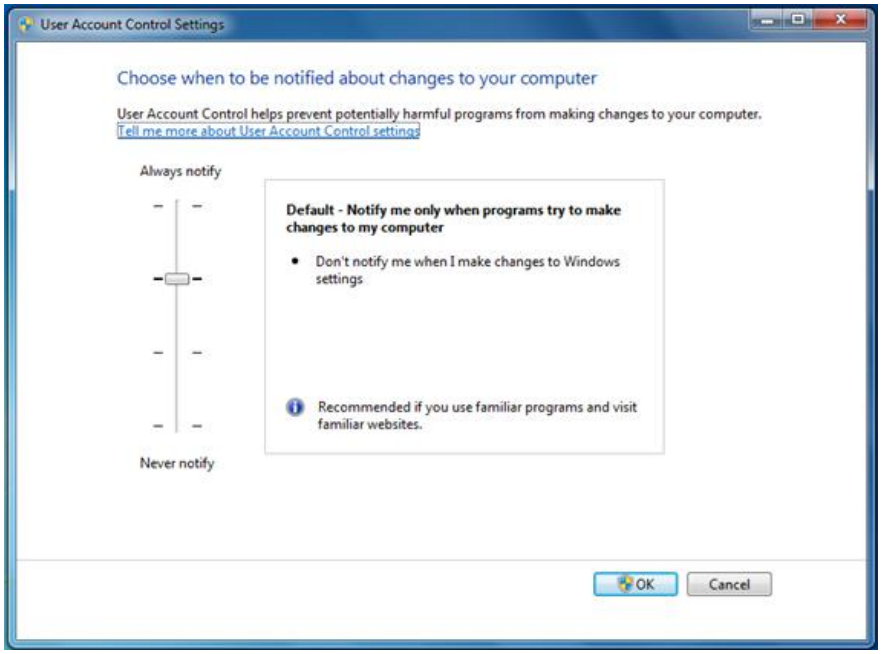

Figure 2: Adjusting the Level of Security by Manipulating the UAC Settings

The UAC is used to prevent programs or applications from making changes to your computer operating system. It works by restricting access within the OS core, and then providing details to the user about the programs attempts to install itself, or further configure the OS. This is helpful in that it will give you a chance to verify what the program is doing, and be able to act on it if it is something you do not want it to do. The UAC was first incorporated with Windows Vista, but since it could not be turned off, was deemed 'annoying' at best. It was frustrating users who could not seem to get around it.

Windows developers also had a lot of trouble coding because of UAC restrictions and needed workarounds. Now, with Windows 7, the UAC can be turned off completely removing that level of security to provide more flexibility and choice.

To keep your system secure, it is recommended that you do not turn off the UAC completely or if you do for any reason, remember to turn it back on. .

Installing and Hardening Windows 7

Windows 7 is secure by design. When deploying it, it is always recommended that you do a fresh install of the operating system on newly purchase (or renovated), compliant hardware and then harden it. System hardening is the process of increasing the level of security on your freshly installed base operating system (OS) by configuring needed security settings, removing unneeded software and adjusting advanced policy settings.

You need to do a little planning when it comes to the hardware selection for Windows 7, because if you want to use virtualization, Windows Trusted Platform Module (TPM) Management and other features such as BitLocker, you will need to purchase the correct hardware for it to function.

Once your OS is installed correctly and basically configured, the process of hardening can take place. Does it always need to be a new installation of Windows, or can you harden a system already running and in use? Yes, you can technically harden any system that is already installed and being used, but before you do, you should first familiarize yourself with it, analyze it, examine it and of course, audit the current security levels configured and in use. It doesn't make sense to harden something that was already compromised. You also may not know how the application of security will affect the production system whether at use in the home, or in a corporate environment. Sometimes duplicate systems are set up in order to test which takes time and resources but well worth it to find and avoid problems that may occur with your design and deployment. You may cause more harm than good if you do not know how security settings changes or the templates will affect services on a production system. For example, you may apply security to a system and through strict firewall filtering changes, remove functionality from a program that you have installed and use – it may use a specific port that is now closed off by the firewall which will cause the connectivity to fail. This may cause adverse effects if the application was something used for business and was needed for productivity and may take some time to discover and correct. This is why it's simply easier to install Windows 7 fresh, and then harden it as it takes place extremely quickly and you can verify that security remains tight until you deploy it. You can also make the process quicker, especially if using a virtual machine (VM) or VHD file] which give you options to have multiple instances of your desktop running for virtual failover or quick restoration and recovery if the redundancy option is not used. Since virtualization simplifies the installation process when creating cloned images for backup purposes, you can restore your desktop easily and within a few minutes. We will cover virtualization again later in the article. If failover is enabled and configured, the desktop user may not even experience an outage at all if virtualized.

You can harden the system, and then access your secure data through shared storage, databases and repositories – and all at high speed, with failover and redundancy options which will not only keep it secure, but separate from the data in which you access. If you plan correctly, you can create an snapshot of a fully prepped, configured, secured and updated version of Windows and in the possibility of disaster, restore your systems image back to your hardware in 1/3 the time it takes to do it without imaging or virtualization cloning. Then, once you restore the base OS, you can reattach to the shared storage to access data.

So, once you install Windows, what are the actual steps taken to harden it? And, is there a specific order to choose from? If there were an organized set of installation and hardening steps, they would be in the basic order of installation, removing anything not used, updating the system, applying basic security to it and then getting it backed up for quick restoration when needed, as seen in the following list :

- **Step 1** - Installation of Base OS selecting any options during installation the increases security and not selecting unneeded services, options and programs.
- **Step 2** - Installation of any Administrator toolkits, security tools and needed programs.
- **Step 3** - Remove services, programs and unneeded software. Disable or remove unused user accounts or groups.
- **Step 4** - Service Pack update, hot fixes and service packs. Update all installed programs as well.
- **Step 5** - Run security audit (scanner, template, MBSA, etc) to assess current security level
- **Step 6** - Run System Restore and create a restore point. Backup and Restoration application for disaster recovery.
- **Step 7** - Backup the OS with a way to quickly restore it in the event of disaster.

This list is a simple guide. You can add more steps and extend this list further. This list is not definitive, but a good start in getting an idea of where to start when applying security to Windows 7 after a base installation. If completing a fresh install of Windows 7, then the next step is to remove any unwanted software, services, protocols and programs that you do not want or need running on it. This can be done easily in the Control Panel.

Next, you can go into the Control Panel and secure who is allowed to use the computer in the User Accounts applet. Here, you should remove any account that you do not need, or just disable it. Of course, be careful with the default users and groups, some of which are tied into your services that run, how your data is accessed and so on. You can always disable an account easily as well if concerned about removing it. Another technique used by most security professionals is to leave the local Administrator account in place and audit it for any attempts at using it, or the domain's administrator account which is even more important to secure and audit. It is common practice to not use the default accounts when managing a large scale Microsoft network of systems and set up new administrator accounts that can be traced if need be. By auditing this default accounts and using a newly made account with administrator privileges associated with it, you increase

security two-fold. One, you find out if someone is trying to get into your machine using the default accounts when nobody should be. If audited, you can see the attempts and when they occur. This application of security to an account is known as a honeypot and helpful in finding possible attempts by others trying access your system. Two, you take away half of the equation when someone is attempting to crack your account via basic credentials, such as a username and password combination. If you take away the easy to guess username credentials, then you are only left with a password which can be configured in a way to where it's nearly impossible to crack. If you set up the default accounts as honeypot, you could create a nearly impossible to crack password and limit it to do next to nothing if compromised so that if it is compromised, there is little to nothing that can be done with it. You should change all the passwords for the default accounts from their currently configured defaults as well. Use password selection best practices when securing these accounts and audit them completely. You should also configure a policy that makes end users looking to change passwords go through a process where they will only be allowed to change it if they select a new password that is strong and not easily hacked. This is just one hardening tip that provides other benefits, such as the ability to find your attacks through logging and auditing.

In Windows Server 2008, you can install 'core' functionality which is a hardening process applied to the system during actual installation. When installed, the server will only run with the minimal functionality you desire, thus reducing your risk of being subjected to security exploits. Windows 7 can be hardened but does not have an install option like 2008 that simply locks down the system upon installation. To harden Windows 7, you need to apply policies, templates or manually configure the security settings as needed.

So, that being said, how do you start to lock down and secure Windows 7? Well, the easiest way start the process of locking down the system is by using the Start menu to search for anything related to security stored within the system and indexed. To do this, simply click on the Start button to open the Start menu. Then, type the keyword 'security' in the Search Programs and Files field. Figure 3 shows the Start menu options based on the 'Security' keyword search.

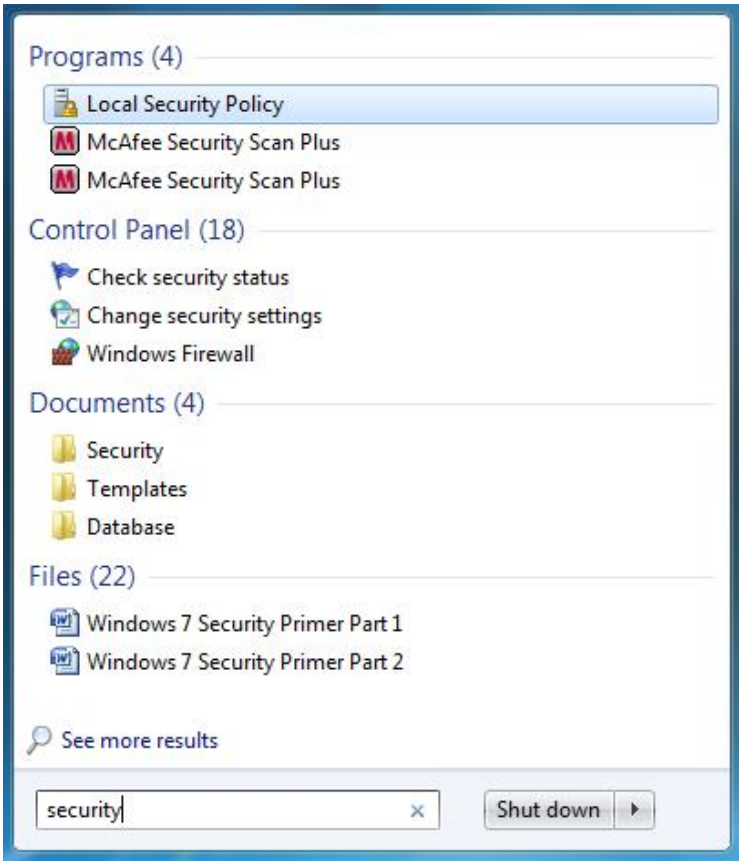

Figure 3: Finding and then Viewing Security Options within the Start Menu

Here, you can see that Programs, Control Panel applets (or actions), Documents and Files are selected and organized for easy viewing and accessibility. In short, Local Security Policy (if selected) is a policy editor that allows you to view and configure the security policies of your system. The Local Security Policy editor can be seen in Figure 4. Here, you can make adjustments to any policy based setting on your operating system.

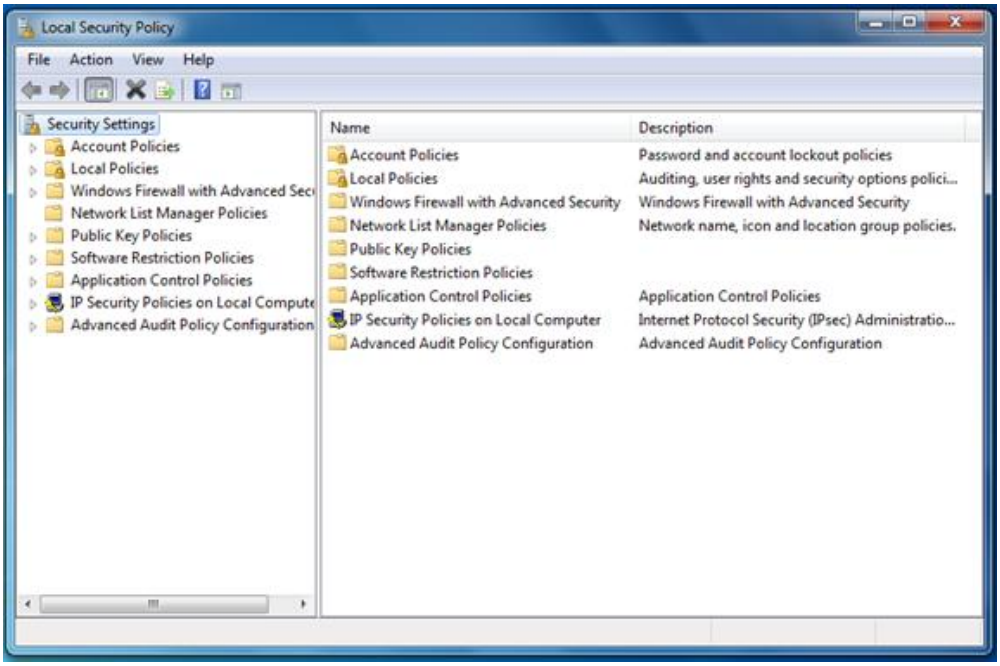

Figure 4: Viewing and Configuring Security with Local Security Policy

Tip – for full policy control, you should use Windows 7 with Windows Server products, such as Windows Server 2008 R2. If you do, then you can use Active Directory (AD) and Group Policy.

If you wanted to locally set up auditing of a specific event (such as system logon and off), then you can specify that action in the Local Security Policy console (Figure 4). In the Control Panel, you can go to the Administrative Tools applet to find the Local Security Policy editor, or simply search for it in the Start menu. When Windows 7 is used with Active Directory, you can use Group Policy which is a robust service that allows you to customize, manage and deploy settings and preferences as well as to deploy software with ease, but you will need to connect Windows 7 to an active domain and manage it correctly in order to benefit.

If you need to configure policy-based security, this is the easiest way. You can also find many of the tools you need for security configuration in the Control Panel and or in a custom MMC you design and deploy. The Microsoft Security Center (Windows Vista, XP) was used to centralize most security functions in the past. This has been replaced with the Action Center, and security actions are now easily found, viewed and acted upon with your permission. For example, as seen in the Start menu (Figure 3), the 'Check security status' action when selected produces a list of security configurations that Windows 7 recommends you act on, such as updating your system, or a program such as antivirus (AV). Once selected, you will be sent to the Action Center to take care of the open issues that need your attention.

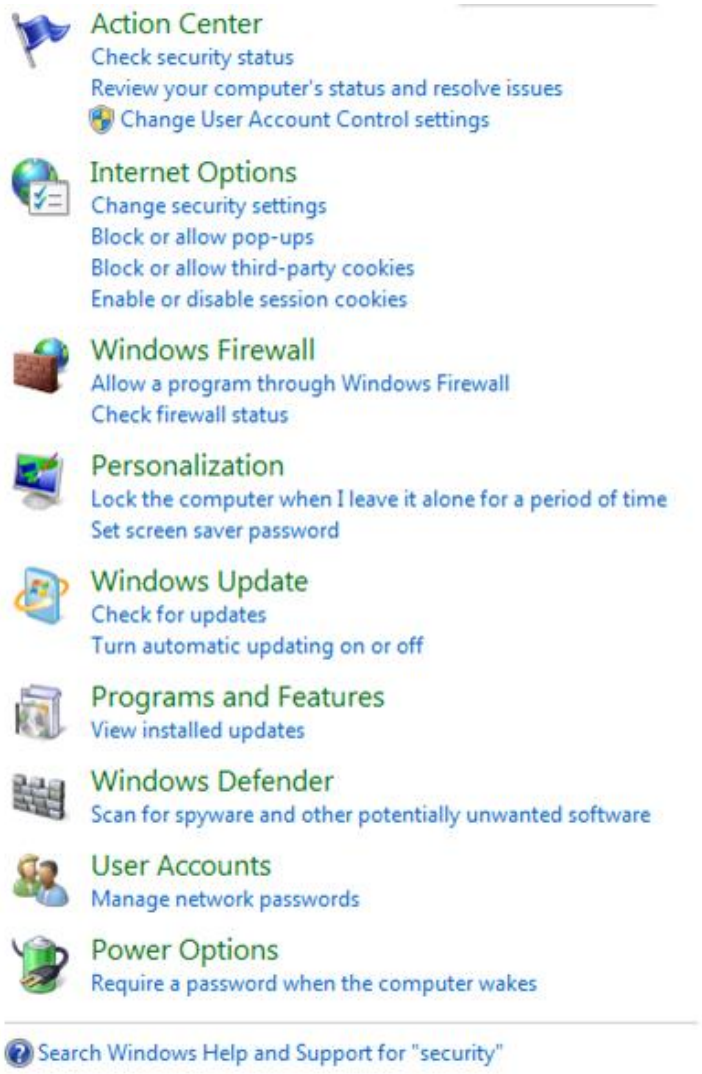

Figure 5: Configure Security Actions and Control Panel Applet Options

Figure 5 shows the security actions found within the Control Panel that you can act on. If you click the Start menu, type security and click on the Control Panel link, you will be given a list of actions and security configurations that you can customize immediately in one easy to find and access list.

Once in the Action Center (or if viewing lists of actions), you can simply go down the list and configure each one as you see fit. This is a brief overview of the security options that can be configured in the Action Center list:

1. **Action Center** – The Action Center replaces the Security Center. The Action Center is where you can specify actions that the OS can perform. With your permission, the actions can take place. Here you will be told if you are missing an Antivirus update as an example. You can access the center to perform security related operations as needed.

2. **Internet Options** – Web browsing of any kind opens the door to Internet-based risks. If you use a proxy server, utilize Web filtering (and monitoring) and keep your OS updated with the latest hot fixes, you may still wind up in a situation where your security is compromised. Within the Internet Options Control Panel applet, you can specify zones for safety, allow only specific URLs to be accessed, deploy advanced security settings in the Advanced tab and much more. The browser itself has a Phishing filter that will prevent Phishing attacks and other configurable options such as InPrivate Browsing, which when selected will prevent the storage of your personal information, particularly helpful when using a computer at a public Kiosk.
3. **Windows Firewall** – Like any other software or hardware-based firewall, Windows Firewall can deflect basic attacks by default, and be configured granularly for a high level of control over what can enter and exit your computer system when connected to a public or private network. By going to the Control Panel and selecting Windows Firewall, you will have access to most firewall configuration settings. You can click on the Advanced settings link in the dialog box to access the Firewall with Advanced Settings and configuration options. With Windows 7, you can also deploy multiple Firewall Policies simultaneously and use the new Domain designation for easier Windows-based firewall configuration and management.
4. **Personalization** – Personalization options are where you can alter the way Windows looks, but it's also where you configure a screensaver password if desired. If running Windows 7 in the enterprise, users should be taught to lock their workstations whenever they leave their desk or issued a policy setting that does it automatically after a period of inactivity, however if forgotten about, a screensaver configured to require logging in again can prove helpful. At home, this may be your best line of defense if you walk away from your system and forget to lock it.
5. **Windows Update** – All software releases require some level of patching. You can prepare, test and attempt to develop perfect software but you can not account for everything. Also, new updates and releases also require updates to your operating system over the lifetime of the current OS version. Because there are advancements in the system, requirements needed for other developing technologies, new security vulnerabilities uncovered and driver updates for better performance and functionality required, there will always be a need for Windows Update. Windows (and Microsoft) Update, or enterprise versions of patch management (WSUS, etc.) are used for centralized control and deployment of updates. These tools are used to control, keep track of and monitor your current and future update needs. Configure to have it do it for you automatically, or get in the habit of doing it manually because it's really important that you do. If you do not patch your OS as recommended (and sometimes required), you may be subject to attack.
6. **Programs and Features** – Other than checking for and seeing what Windows Updates are installed, you should check to see what you have installed on your system often, especially if you work on the Internet and/or download software from Internet-based Web servers. For example, by installing a simple Java update,

if you did not read the screens carefully during install, you may have also installed a toolbar on your system which integrates into your Web browser. Now, there is tighter control over this, but regardless, you should still check from time to time to see what is currently installed on your system.

7. **Windows Defender** – Spyware is software that is used primarily for illicit marketing purposes, and does other things such as deliver a direct payload, redirects your browser or sends back information on your actions. Although Antivirus software picks up some of this, Windows Defender (or other Spyware-removal applications) can be counted on to clean up the rest. Cookies, although harmless by nature can sometimes be manipulated for the wrong reasons. Make sure Windows Defender is updated often with new definition files and its needed updates to ensure you are scanning for all of the latest Spyware currently known about. SpyNet is also a community that Microsoft watches over to learn about, talk about and prevent the spreading and damage produced by Spyware.
8. **User Accounts** – Managing user accounts is the core to securing access to your computer as well as everything that runs within it. For example, if you create a new user account and assign it to the Administrators group, you have full access to the computer system. If you configure the account as a standard user, then the permissions granted will be very restrictive and will only allow the user to do specific things. You can also configure a password which when created with a minimum password restriction or policy, enforces the user to create a difficult to crack credential set to thwart basic password cracking attempts. Once Windows Server 2008 and Active Directory is deployed, you can access a domain that when once joined, will allow you to configure granular NT File System (NTFS) permissions to folders and files as well as other shared resources like printers.
9. **Power Options** – The Power Options Control Panel applet is where you can configure the default behavior of the Operating System when unplugged, closed or goes to sleep. The security configuration to set is that a password be required when the computer awakes from a sleep state. Anytime you can enable the use of access control, you should consider it.

So, if you need to apply security to Windows 7, the Start menu can serve as a good way to get started in the basic hardening of your system and open the door to the available tools you can use. There are many options here you can use to harden your Windows 7 system, especially within the Control Panel. Using the Start menu is also an easy way to get a security baseline of your system after initial installation. A tip you can try is to set up a baseline after the initial installation and configuration of your system, which would require you to configure all security options, applications, as well as download hot fixes and updates, and then backup the entire system image with System Restore and/or a system imaging utility. Now you have a snapshot of your system in a fresh state in case you need to revert back to it later. You can make a restore point which could be used if the system is compromised, allowing you to again have a basically configured system with basic security applied. We will cover System Restore options in the Disaster Recovery section of this article.

The Start menu can also help provide information on security related documentation on your system. This is helpful when searching for a document such as a security policy, or a hardening checklist or template.

You can quickly harden Windows by downloading the tools and documentation directly from Microsoft and go down the list of recommendations provided. For example, if you wanted to configure a basic level of security for Windows 7, you could easily download the baseline security template for use, run it and have most of your security settings adjusted for you. Figure 6 shows the Windows 7 Security Baseline Settings template with tabbed spreadsheet (workbook) entries for user account auditing, BitLocker and more. Visit the Reference Links section at the end of the article to gain access to it.

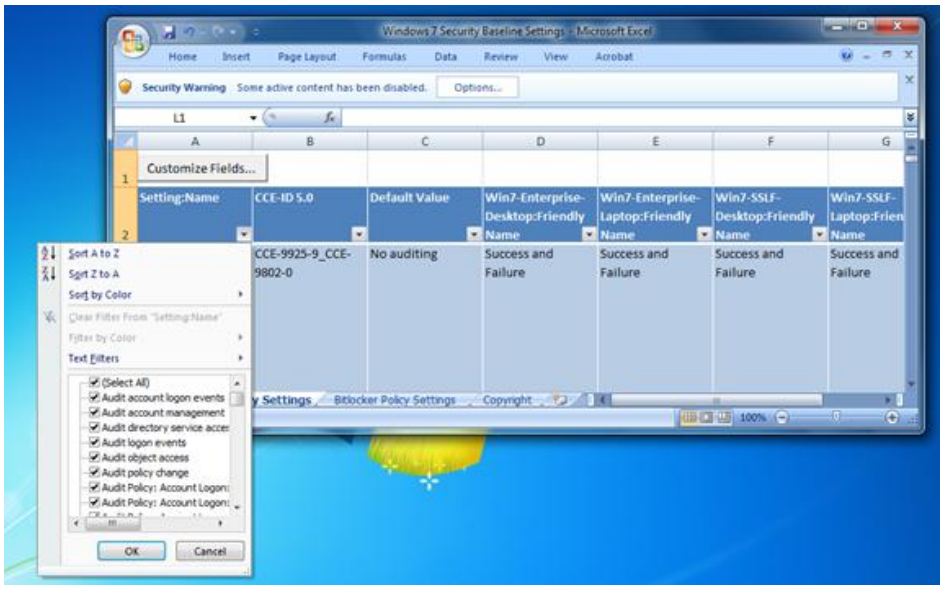

Figure 6: Configuring Baseline Security from Microsoft Templates

Take note of the 'Security Warning' option on the top toolbar (ribbon) of Microsoft Office Excel 2007 which prevents you from using the template by disabling the Macro until you attend to Security Warning as seen in Figure 6. Here, Security Macros have been disabled and are required for the application of this template. This is a perfect example of security vs. flexibility. To have flexibility in this instance, you need to turn off or limit the level of security applied in order to achieve it. Manually selecting the option to run, or disabling the protection, run the Macro and then boost the level of security once more to keep security in place will get the template installed.

Now that your system is ready to go and you have basic security features configured, you should now consider how to manage it, as well as monitor for intrusion, malware and for other problems found within the logs.

You should also note that Windows 7 has an option available called XP-mode, commonly used for resolving application compatibility issues with older XP-based applications. As we have discussed the topic of virtualization earlier, when considering using XP-mode, you are installing Virtual PC on Windows 7 and running an instance of XP on Virtual

PC. If you use XP-mode, make sure harden any VMs running on Virtual PC the same way you harden the base OS. This includes AV protection, policy lockdown and Service Pack and software updates to name a few. You can provide a level of security through virtualization, but not completely so you still need to take hardening steps, even if virtualization is used.

Reference Links

1. Windows 7 Security Features
2. Windows 7 Security Enhancements
3. target=_blankWindows 7 Security TechNet Blog
4. target=_blankWindows 7 Security Checklist
5. Ten Things IT Professionals Should Know About Windows 7
6. Microsoft Malicious Software Removal Tool and Safety Assessment Scan
7. Windows 7 System Requirements
8. Virtual PC and XP-Mode
9. Windows 7 Compatibility Center
10. Windows Performance and Hardware Compatibility
11. AppLocker
12. Download and Install Microsoft Security Essentials for Windows 7
13. BitLocker Drive Encryption Step-by-Step Guide for Windows 7
14. Windows Trusted Platform Module Management Step-by-Step Guide
15. Microsoft Security Compliance Management Toolkit
16. Windows Server 2008 Security Compliance Management Toolkit
17. Enterprise Security Management with Forefront
18. Network Access Protection (NAP)
19. Cisco Network Admission Control (NAC)
20. Introduction to DNSSEC
21. DNSSEC Components and Terminology
22. The Trustworthy Computing Security Development Lifecycle (SDL)
23. Common Criteria Certification: Microsoft Windows Platform Products
24. Responding to IT Security Incidents (Incident Response Planning)
25. An Introduction to Kernel Patch Protection
26. Data Execution Prevention
27. Windows Integrity Mechanism Design
28. Understanding and Working in Protected Mode Internet Explorer
29. Strategies for Managing Malware Risks
30. Security Risk Management Guide and Toolkit
31. Security Monitoring and Attack Detection
32. Windows 7 and Windows Server 2008 R2: Controlling Communication with the Internet
33. Leverage Windows 7 Security in Business Environments
34. Windows 7 Security in the Enterprise
35. Request for Comments (RFC) Search

Articles by Rob Shimonski

36. http://www.windowsnetworking.com/Robert_J_Shimonski/
37. http://www.windowsecurity.com/Robert_J_Shimonski/
38. http://www.virtualizationadmin.com/Robert_J_Shimonski/

Official site of Microsoft:

39. http://technet.microsoft.com/en-us/library/cc507844.aspx